UNITED STATES DISTRICT COURT
IN THE DISTRICT OF SOUTH CAROLINA
ROCK HILL DIVISION

Sloan Financial Group, LLC, Plaintiff, v. Marcus P. Coe and Allied Insurance Marcus Coe Agency, LLC, Defendants.	Civil Action No.: 0:09-cv-02659-CMC OPINION AND ORDER ON MOTION FOR PARTIAL SUMMARY JUDGMENT

This matter is before the court on motion for partial summary judgment filed by Defendants Marcus P. Coe ("Coe") and Allied Insurance Marcus Coe Agency, LLC ("Agency"). Dkt. No. 65. Defendants seek summary judgment on the claim for violation of the Computer Fraud and Abuse Act ("the CFAA"), 18 U.S.C. § 1030 *et seq.*, asserted by Plaintiff Sloan Financial Group, LLC ("Sloan"). *See* Dkt. No. 1 (complaint filed on October 12, 2009). Defendants further move for dismissal of the remaining state law claims and counterclaims pursuant to 28 U.S.C. § 1367(c) in the event their motion for partial summary judgment is granted.

For the reasons set forth below, the court grants Defendants' motion for partial summary judgment and declines to exercise supplemental jurisdiction over the remaining state law claims and counterclaims. The state law claims and counterclaims are, therefore, dismissed without prejudice.

STANDARD

Summary judgment is appropriate "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). It is well established that

summary judgment should be granted "only when it is clear that there is no dispute concerning either the facts of the controversy or the inferences to be drawn from those facts." *Pulliam Inv. Co. v. Cameo Properties*, 810 F.2d 1282, 1286 (4th Cir. 1987).

The party moving for summary judgment has the burden of showing the absence of a genuine issue of material fact, and the court must view the evidence before it and the inferences to be drawn therefrom in the light most favorable to the nonmoving party. *United States v. Diebold, Inc.*, 369 U.S. 654, 655 (1962). When the nonmoving party has the ultimate burden of proof on an issue, the moving party must identify the parts of the record that demonstrate the nonmoving party lacks sufficient evidence. The nonmoving party must then go beyond the pleadings and designate "specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e); *see also Celotex Corp. v. Catrett*, 477 U.S. 317 (1986).

A party "cannot create a genuine issue of material fact through mere speculation or the building of one inference upon another." *Beale v. Hardy*, 769 F.2d 213, 214 (4th Cir. 1985). Therefore, "[m]ere unsupported speculation . . . is not enough to defeat a summary judgment motion." *Ennis v. National Ass'n of Bus. & Educ. Radio, Inc.*, 53 F.3d 55, 62 (4th Cir. 1995).

FACTS & BACKGROUND

Sloan, a business located in Clover, South Carolina, provides insurance, financial planning, and tax preparation services. Dkt. No. 1 ¶1. Sloan hired Coe in June of 2006 to sell various forms of insurance. Dkt. No. 74-1 at 3. Sloan provided Coe with an office and desktop computer with internet access and emailing capability to enable him to perform his job responsibilities. *Id.* at 4-5. Sloan also paid to have Coe appointed to sell insurance for a variety of different carriers. *Id.* at 5-7.

Sloan's Client Information Policies. On December 4, 2007, Sloan circulated an office

memorandum restricting employees' use of client information. This memorandum stated, "[i]t is imperative that all office personnel understand that no client information be taken out of the office. . . . This information includes electronic data (laptops, CDs, disks, flash-drives, emails), files, paperwork, etc." Dkt. No. 68-3. Coe acknowledged receipt of this policy in December 2007.

Sloan established a more detailed confidentiality policy relating to client and proprietary information on December 1, 2008 when it issued a new employee handbook. Dkt. No. 68 at 2. This policy provides, in pertinent part, that "[i]nformation concerning [Sloan's] clients is confidential. . . . Confidential information may not be released by anyone without proper authority, nor may it be used for personal gain." Dkt. No. 68-4 at 32. The handbook also includes a section on access to and use of Sloan's computer systems, providing that "[a]ll computers, related equipment and computer accounts . . . are provided as tools to assist [employees] in performance of [their] job-related duties and responsibilities." Dkt. No. 68-4 at 20. Coe was issued a copy of the employee handbook containing these policies but refused to sign the handbook because "there were some things in [it] that [he] didn't agree with." Dkt. No. 74-1 at 13.

Coe's Access to Information About Sloan's Clients. In October 2008 (after issuance of the December 2007 memorandum but before publication of the employee handbook in December 2008), Coe used his work computer to email a document from his work email address to his personal email address. Dkt. No. 74-2 at 2. The document was an Excel spreadsheet Coe had created containing information about 39 of Sloan's clients. *Id.* at 3-4. In November 2008, Coe sent another spreadsheet from his work email to his personal email address, which contained information about 107 of Sloan's clients. Dkt. No. 74-3.

On or around December 17, 2008, after issuance of the handbook, Coe accessed Sloan's

computer system to search phrases such as "agent of record change" and "broker dealer transfer" on an electronic database belonging to Harleysville Insurance Company ("Harleysville").[1] In January 2009, Coe again accessed the Harleysville database from his work computer to view quote details about Sloan's clients including customer names, policy numbers, renewal status, premium amounts, and renewal dates. Dkt. No. 74-6.

Also in January 2009, Coe ordered, at Sloan's expense, Choice Point reports on individuals who never became clients of Sloan but who later became clients of Coe when he opened a new insurance agency later that year.[2] Dkt. Nos. 1 ¶19 & 74-1 at 42-61. Coe's access to the Choice Point program was provided and authorized by Sloan. Dkt. No. 74-1 at 42-43.

Coe Forms a New Agency. The above-referenced transmissions and searches occurred during a period when Coe was dissatisfied with at least some aspects of his employment. This dissatisfaction began when Sloan modified its employees' commission structure in October 2008. *Id.* at 10-11. Beginning in December 2008, Coe began contemplating opening his own insurance agency. *Id.* at 12. On January 21, 2009, ten days before tendering his resignation from Sloan, Coe registered his new agency, Allied Insurance Marcus Coe Agency, LLC, with the National Association of Insurance Commissioners.[3] Dkt. No. 72-8. Coe tendered his resignation from Sloan

---

[1] Coe describes the database as belonging to the insurance carrier, Harleysville. Coe was given access to this database through a password provided by Sloan because Sloan is a broker for Harleysville's products. Dkt.No. 74-1 at 33. Access to the database allowed Coe to view the status of clients and customers. *Id.* Sloan does not dispute this description of the Harleysville database.

[2] Coe describes Choice Point as a company through which one orders claims reports. Dkt. No. 74-1 at 42. An insurance company would order a report through Choice Point to see if a new client meets the company's guidelines. *Id.* at 43. Sloan does not dispute this description of Choice Point.

[3] The date listed on the National Association of Insurance Commissioners' form is January 21, 2008. Sloan contends and the circumstances suggest that this year (2008) is a typographical

on or about January 30, 2009 and began running his own insurance agency shortly thereafter. Dkt. No. 66 at 4.

Sloan alleges that Coe used the information he gleaned from Sloan's computer system, his searches of Harleysville's database, and the Choice Point reports to recruit clients for his new Agency and actively take business away from Sloan. For purposes of summary judgment, the court accepts these inferences as true.

Procedural Background. Defendants moved to dismiss Plaintiff's CFAA cause of action on March 15, 2010. Dkt. No. 51. Then as now, Defendants argued that the alleged actions do not fall within the scope of the CFAA. *Id.* In light of the split of authority as to the scope of the CFAA, outlined below, the absence of Fourth Circuit authority on the issue, and the presence of other claims and counterclaims, the court denied the motion to dismiss without prejudice to a post-discovery summary judgment motion raising the same arguments. Dkt. No. 62. Defendants now raise the same arguments in support of their motion for partial summary judgment.

DISCUSSION

I. THE CFAA CLAIM

Sloan's only federal claim is founded on 18 U.S.C. § 1030 *et seq.*, the CFAA. Dkt. No. 1 ¶¶ 30-39. Although the CFAA is primarily a criminal statute generally intended to deter computer hackers, it permits private parties damaged as a result of a violation to bring a civil action assuming sufficient injuries. *A.V. ex rel Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009). Specifically, the statute provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action" when damages or losses meet or exceed $5,000

---

error. For the purposes of this order, the court accepts Sloan's explanation as true.

in one year. § 1030(g).[4]

Sloan alleges that Coe violated the CFAA through the following three categories of action:

(1) transmitting two spreadsheets of Sloan's client information from his work email address to his home email address;

(2) conducting searches on the Harleysville database for his own benefit; and

(3) at Sloan's expense, ordering Choice Point reports on individuals who never became clients of Sloan's, but later became clients of Coe's new Agency.

Sloan asserts that by taking these actions Coe violated sections 1030(a)(2)(A), 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(B) and (C) of the CFAA. The sections provide a remedy against a party who:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains
>
> (A) information contained . . . in a file of a consumer reporting agency on a consumer . . . ;[5]
>
> ***
>
> (C) information from any protected computer;
>
> ***
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . .;
>
> (5) (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

[4] Section 1030(g) allows for a civil action upon a showing of one of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Plaintiff is relying on subclause (I) of subsection (c)(4)(A)(i) which requires a showing of "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." § 1030(c)(4)(A)(i)(I).

[5] Sloan alleges that Coe violated section (a)(2)(A) by ordering the Choice Point reports because Choice Point provides consumer reporting agency information.

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

18 U.S.C. § 1030(a)(2)(A); (a)(2)(C), (a)(4), and (a)(5)(B)-(C).

Liability under the relevant sections requires, as a predicate, showing that an individual acted "without authorization" (all five sections) or "exceed[ed] authorized access" (three sections). For the reasons set forth below, the court concludes that Sloan has not proffered evidence sufficient to establish that Coe acted either without authorization or in excess of authorization when taking any of the actions alleged in this case.

In order for Sloan's CFAA claim to succeed, the court would have to conclude that an employee acts "without authorization" or "exceeds authorized access" when he accesses a computer or protected computer with an intent that is contrary to the interests of his employer. The plain meaning of the statute does not support that interpretation.[6]

---

[6] The court recognizes that there is a split of authority on this question. Under a line of cases referred to as the *Citrin* line, the determination of whether "authorization" exists turns on whether the person accessing the information breached a duty of loyalty. *See Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). The Seventh Circuit, in *Citrin*, held that an employee who violates the duty of loyalty by acting adversely to his employer's interests loses his authorization to access the employer's protected computer. *Id*. at 421.

Four other federal circuits have held or noted that an employee acts "without authorization" or "exceeds authorized access" under the CFAA when he either acts disloyally to his employer or acts in contravention of his employer's policies governing computer usage. *See, e.g., United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) ("[A]n employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business"); *United States v. Salum*, 257 Fed. Appx. 225, 230-31 (11th Cir. 2007) ("[A]lthough [the defendant] may have had authority to access the [computer] database, there was sufficient evidence to establish that . . . [the defendant] exceeded his authority by accessing it for improper purpose."); *P.C. Yonkers Inc. v. Celebrations The Party and Seasonal Superstore LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (recognizing that the CFAA's reach extends to actions against "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001) ("We conclude that because of the broad confidentiality

A. Meaning of "Without Authorization"

Sloan alleges that Coe's actions in emailing spreadsheets, searching Harleysville's database, and ordering reports from Choice Point were all "without authorization" because Sloan had confidentiality policies in place that prohibited employees from removing client information from the office or using client information for their personal gain. The CFAA creates liability when an individual "accesses" a computer or a protected computer "without authorization." The company policies at issue in this case restrict how a Sloan employee can use data. They do not affect an employee's ability to access that data in the first place. Because liability under the CFAA is based on access not use, Coe's intended use of Sloan's client data does not create liability under the CFAA. *See, e.g., LVRV Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009) (interpreting "without authorization" as being without permission or having permission rescinded, and concluding that an employee's intended later use of information he has permission to access has no bearing on "authorization" to access it under the CFAA).[7]

---

agreement[,] appellants' actions 'exceed[ed] authorized access.'"). The holdings in these cases turn on the employees' purposes for accessing the information and whether or not those purposes were proper in light of employers' policies.

[7] While the Fourth Circuit has not ruled on the issue, recent district court opinions within the Fourth Circuit suggest "authorization" does not turn on an employee's intended use of information in a manner that is adverse to employer interests or policy. *See Océ North Amer., Inc. v. MCS Servs., Inc.*, No. WMN-10-CV-984, 2010 WL 3703277, at *4 (D. Md. Sept. 16, 2010) (holding that while an employee remained employed by the company, he had authorization to use computers and computer software and that "copying software onto his own laptop may have been a violation of his employment agreement, but that does not constitute a violation of the CFAA"); *Cvent, Inc. v. Eventbrite, Inc.*, No. 1:10-cv-00481, 2010 WL 3732183, at *4 (E.D. Va. Sept. 15, 2010) (noting that "a mere allegation that a defendant 'used the information [which it had been given lawful authority to access] in an inappropriate way' did not state a claim for relief [under the CFAA]") (quoting *State Analysis, Inc. v. Amer. Fin. Servs., Assoc.*, 621 F. Supp. 2d 309, 317 (E.D. Va. 2009)).

Emailing Spreadsheets. It is undisputed that Coe was employed by Sloan when he allegedly created spreadsheets of client data and emailed them from his work email account to his personal account. During his employment, Coe was given a computer and email services in order to perform his duties as an employee. Sloan has not proffered any evidence that Coe was prohibited from accessing any of the client data that Coe gleaned from his computer to make the spreadsheets at issue or that he was unauthorized to access Sloan's email service. Therefore, Coe was not acting "without authorization" when he created the spreadsheets of client data or when he emailed them.

In reaching this decision, the court assumes without deciding that Coe violated Sloan's policy prohibiting employees from removing client information from the office when he sent the spreadsheets to his personal email address. This policy did not, however, preclude or limit access to the client information by employees. Moreover, the allegedly improper action of sending the spreadsheets was a distinct action from access, which was authorized. In short, whether or not it was a violation of company policy, emailing the spreadsheets did not involve accessing a computer "without authorization" under the CFAA.

Access of Third Party Databases. Sloan has failed to proffer evidence that searching the Harleysville database and ordering reports from Choice Point constituted unauthorized access as required for liability under the CFAA. First, from Sloan and Coe's perspective, this access was authorized because Sloan provided Coe with the passwords he needed to access the Harleysville database and to order Choice Point reports. Sloan has not proffered any evidence that Coe's access violated either its policy regarding access to these third party databases or any policies of

Harleysville or Choice Point regulating access to the databases.[8] Therefore, there is no evidence to support the assertion that Coe acted without authorization when he accessed these databases. The court therefore finds that the evidence does not support a finding that access to these third party databases was "without authorization."

B. Meaning of "Exceeds Authorized Access"

In the alternative, Sloan argues that Coe acted in excess of authorized access.[9] While the CFAA does not define "authorization," it does define "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." §1030(e)(6).

As stated above, Coe was authorized to use his work computer to access information. Therefore, for Sloan's argument to succeed, it would have to show that due to company policy, Coe was not entitled to obtain (1) the information about Sloan's clients that appeared in the emailed spreadsheets or (2) the information he obtained from Harleysville and Choice Point. Sloan, however, has only proffered evidence of company policies that limit an employee's use of information, and not policies that limit an employee's right to access or obtain information. Therefore, the court finds that Sloan has not proffered evidence that Coe exceeded authorized access by performing any of the alleged actions.

---

[8] In reaching this conclusion, the court recognizes that the CFAA may not impose an "ownership or control requirement." *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004). The language of the statute allows a party to seek a civil remedy if it experiences loss or damage due to information obtained from *any* protected computer. 18 U.S.C. § 1030(a)(2)(C) and (g) (emphasis added).

[9] This is only applicable to three of the five sections Sloan alleges Coe violated (sections (a)(2)(A), (a)(2)(C), and (a)(4)).

Sloan argues that this court should follow the Fifth Circuit's interpretation of "exceeds authorized access" as expressed in *United States v. John*. 597 F.3d at 273 (*supra* n.6). That opinion states that "when an employee knows that the purposes for which [he] is accessing information in a computer is . . . in violation of an employer's policies . . ., it would be 'proper' to conclude that such conduct 'exceeds authorized access.'" *Id.* Even if the court adopted this interpretation, it would not fit the facts of this case.

Liability under the CFAA, based on an allegation that an employee exceeded authorized access, depends on whether the employee obtained information he was not entitled to access. To the extent an employee's purpose is to violate an employer policy regulating *access* to information, the conclusion of the *John* court would be consistent with the language of the CFAA. But, in this case, Sloan's company policy regulated *use* of information not access to that information. Thus, even if Coe's purpose in accessing the information was contrary to company policy regulating use, it would not establish a violation of company policy relevant to access and, consequently, would not support liability under the CFAA.[10] The court concludes that Coe did not exceed authorized access in taking the actions alleged in this case.

Regardless of whether analyzing Coe's actions as unauthorized or in excess of authorization, the court considers that the CFAA is primarily a criminal statute enacted by Congress to deter

---

[10] In reaching this conclusion the court joins a "critical mass" of cases holding that CFAA liability depends on actions taken by an employer in authorizing access to information rather than on an employee's purpose or intended future use of that information. *See Lewis-Burke Assoc., LLC v. Widder*, No. 09-302, 2010 WL 2926161, at *5 (D.D.C. July 28, 2010); *see, e.g.*, *Cvent*, 2010 WL 3732183, at *4; *Orbit One Com., Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); *Nat'l City Bank, N.A. v. Republic Mortg. Home Loans, LLC*, No. 09-CV-1550, 2010 WL 959925, at *2 (W.D. Wash. Mar. 12, 2010); *Bell Aerospace Servs. Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010); *ReMedPar, Inc. v. AllParts Medical, LLC*, 683 F.Supp.2d 605, 611 (M.D. Tenn. 2010).

computer hackers and enhance the government's ability to prosecute computer crimes. *Vanderhye*, 562 F.3d at 645. Although there is a civil remedy available, there is no evidence that Congress intended the statute be used to help companies enforce their confidentiality or non-competition policies. *See Nat'l City Bank*, 2010 WL 959925, at *4 ("There is no reason to believe that Congress intended [the CFAA] to create a federal enforcement mechanism for corporate policies regarding document handling and retention."). There are a variety of other legal remedies potentially available to an employer who finds that an employee has misused or misappropriated proprietary or confidential information.[11]

Additionally, where a statute has both criminal and noncriminal applications, courts should interpret the statute consistently. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). The Supreme Court cautions against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants. *See United States v. Bass*, 401 U.S. 336, 347-49 (1971). To interpret "authorization" or "exceeds authorized access" based on an employee's purpose or based on whether the employee's interests were adverse to the interests of his employer at the time of access would expand the reach of this statute well beyond its literal terms. This would be both confusing and antithetical to the rule of lenity which states, a court "will not interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on no more than a guess as to what Congress intended." *U.S. v. Seidman*, 156 F.3d 542, 559 (4th Cir. 1998).

---

[11] *See, e.g.*, Dkt. No. 1 (asserting causes of action for breach of duty of loyalty, misappropriation of trade secrets and confidential and proprietary information, intentional interference with existing business relations, intentional interference with prospective business relations, civil conspiracy, conversion, and unjust enrichment).

C. Conclusion

For the reasons stated above, the court concludes that Sloan has not shown that Coe acted "without authorization" or "exceeded authorized access" in violation of the CFAA. The court, therefore, grants summary judgment in favor of Defendants on the CFAA claim.

II. SUPPLEMENTAL JURISDICTION

Defendants ask the court to exercise its discretion to decline the continued exercise of supplemental jurisdiction over the remaining state law claims and counterclaims asserted in this action. Plaintiff has not filed any opposition to this aspect of Defendants' motion.

The court's jurisdiction over the state law claims and counterclaims is premised on supplemental jurisdiction. *See* 28 U.S.C. § 1367(a). The court may decline to exercise supplemental jurisdiction if it "has dismissed all claims over which it has original jurisdiction." 28 U.S.C. § 1367(c)(3); *see also Shanaghan v. Cahill*, 58 F.3d 106, 109 (4th Cir. 1995) ("The doctrine of supplemental jurisdiction indicates that federal courts generally have discretion to retain *or* dismiss state law claims when the federal basis for an action drops away.").

"[T]rial courts enjoy wide latitude in determining whether or not to retain jurisdiction over state claims when all federal claims have been extinguished." *Shanaghan*, 58 F.3d at 110. The Fourth Circuit has identified several factors for a court to consider when making this determination: (1) "convenience and fairness to the parties," (2) "the existence of any underlying issues of federal policy," (3) "comity," and (4) "considerations of judicial economy." *Id.* (citing *Carnegie-Mellon Univ. v. Cohill*, 484 U.S. 343, 350 n.7 (1988); *Growth Horizons, Inc. v. Delaware County*, 983 F.2d 1277, 1284 (3d Cir.1993)).

Fairness. A motion to dismiss the CFAA claim was filed early in this case. *See* Dkt. No.

23 (motion to dismiss filed December 9, 2009). The court denied this motion without prejudice to a post-discovery motion for summary judgment on the same ground. Therefore, Plaintiff has been on notice that its CFAA claim could be dismissed for over ten months. Additionally, a key fairness consideration is whether any applicable statute of limitations would prevent Plaintiff from refiling the dismissed state law claims in the appropriate state court. *See Ketema v. Midwest Stamping, Inc.*, 180 Fed. Appx. 427, 428 (4th Cir. 2006) ("[T]he dismissal may be an abuse of discretion where the state statute of limitations expired prior to dismissal of the anchor federal claim."). However, 28 U.S.C. § 1367(d) provides that "[t]he period of limitations for any [state law claim asserted under 1367(a)] . . . shall be tolled while the claim is pending [in federal court] and for a period of 30 days after it is dismissed unless State law provides for a longer tolling period."[12] Therefore, the court's dismissal of Sloan's state law claims will not result in Sloan losing the opportunity to have its case considered on the merits by a court of law.

Other Factors. The other factors, likewise, support dismissal. There are, for example, no federal policy or other federal issues remaining. Comity, therefore, favors dismissal because a state court is better suited to handle a matter involving only state law claims. While there may be some loss of judicial economy, that loss should be minimal as the parties may utilize the discovery completed while the matter was pending before this court.

Accordingly, pursuant to 28 U.S.C. § 1367(c)(3), the court dismisses the remaining state law

[12] States are required to give effect to this federal tolling provision so long as the dismissed state law claims were properly asserted in federal court under 28 U.S.C. § 1367(a). *See Jinks v. Richland County*, 538 U.S. 456, 466 (2003) (holding that this section is constitutional even when it tolls the statute of limitations applicable to a cause of action brought against a State's political subdivision and, therefore, implicates sovereign immunity).

claims and counterclaims without prejudice.

CONCLUSION

For the reasons stated above, the court grants the motion of Marcus P. Coe and Allied Insurance Marcus Coe Agency, LLC for partial summary judgment as to the CFAA claim. Under 28 U.S.C. § 1367(c)(3), the court dismisses the remaining state law claims and counterclaims without prejudice.

IT IS SO ORDERED.

s/ Cameron McGowan Currie
CAMERON MCGOWAN CURRIE
UNITED STATES DISTRICT JUDGE

Columbia, South Carolina
November 18, 2010